

EXHIBITS A1-A6 (Part 6 of 13)

Cisco's Documentation	Arista's Documentation	Supporting Evidence In The Record
<p>ip extcommunity-list</p> <p>To create an extended community list to configure Virtual Private Network (VPN) route filtering, use the ip extcommunity-list command in global configuration mode. To delete the extended community list, use the no form of this command.</p> <p>Global Configuration Mode CLI</p> <pre>ip extcommunity-list expanded-list / expanded list-name {permit deny} [regular-expression] / standard-list / standard list-name {permit deny} [rt value] [soo value]</pre> <pre>no ip extcommunity-list expanded-list / expanded list-name / standard-list / standard list-name</pre> <p>To enter IP extended community-list configuration mode to create or configure an extended community-list, use the ip extcommunity-list command in global configuration mode. To delete the entire extended community list, use the no form of this command. To delete a single entry, use the no form in IP Extended community-list configuration mode.</p> <pre>ip extcommunity-list expanded-list / expanded list-name / standard-list / standard list-name</pre> <pre>no ip extcommunity-list expanded-list / expanded list-name / standard-list / standard list-name</pre> <p>Cisco IOS IP Routing Protocols Command Reference (June 10, 2005), at 116.</p>	<p>ip extcommunity-list standard</p> <p>The ip extcommunity-list standard command creates an extended community list to configure Virtual Private Network (VPN) route filtering. Extended community attributes filter routes for virtual routing and forwarding instances (VRFs).</p> <ul style="list-style-type: none"> Route Target (rt) attribute identifies a set of sites and VRFs that may receive routes that are tagged with the configured route target. Configuring the route target extended attribute with a route allows that route to be placed in the per-site forwarding tables that route traffic received from corresponding sites. Site of Origin (soo) attribute uniquely identifies the site from which the provider edge (PE) router learned the route. All routes learned from a specific site must be assigned the same site of origin attribute whether a site is connected to a single PE router or multiple PE routers. Configuring this attribute prevents the creation of routing loops when a site is multihomed. The SOO extended community attribute is configured on the interface and is propagated into BGP through redistribution. The SOO should not be configured for stub sites or sites that are not multihomed. <p>The no ip extcommunity-list standard and default ip extcommunity-list standard commands delete the specified extended community list by removing the corresponding ip extcommunity-list standard statement from <i>running-config</i>.</p> <p>Platform all Command Mode Global Configuration</p> <p>Command Syntax</p> <pre>ip extcommunity-list standard listname FILTER_TYPE COMM_1 [COMM_2...COMM_n]</pre> <pre>no ip extcommunity-list standard listname</pre> <pre>default ip extcommunity-list standard listname</pre> <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1591.</p> <p>See also Arista User Manual v. 4.13.6F (4/14/2014), at 1541; Arista User Manual v. 4.12.3 (7/17/13), at 1365; Arista User Manual, v. 4.11.1 (1/11/13), at 1111; Arista User Manual v. 4.10.3 (10/22/12), at 923; Arista User Manual v. 4.9.3.2 (5/3/12), at 690; Arista User Manual v. 4.8.2 (11/18/11), at 520.</p>	<p>Dkt. 419-10 at PDF p. 176</p>

Cisco's Documentation	Arista's Documentation	Supporting Evidence In The Record
<p>ip extcommunity-list</p> <p>To create an extended community list to configure Virtual Private Network (VPN) route filtering, use the ip extcommunity-list command in global configuration mode. To delete the extended community list, use the no form of this command.</p> <p>To enter IP Extended community-list configuration mode to create or configure an extended community-list, use the ip extcommunity-list command in global configuration mode. To delete the entire extended community list, use the no form of this command. To delete a single entry, use the no form in IP Extended community-list configuration mode.</p> <p>Global Configuration Mode CLI</p> <pre>ip extcommunity-list {expanded-list [permit deny] [regular-expression]} expanded list-name [permit deny] [regular-expression] standard-list [permit deny] [rt value] [soo value] standard list-name [permit deny] [rt value] [soo value]} no ip extcommunity-list {expanded-list expanded list-name standard-list standard list-name}</pre> <p>ip extcommunity-list {expanded-list expanded list-name standard-list standard list-name} no ip extcommunity-list {expanded-list expanded list-name standard-list standard list-name}</p> <p>Cisco IOS IP Routing: BGP Command Reference (2013), at 326.</p>	<p>ip extcommunity-list expanded</p> <p>The ip extcommunity-list expanded command creates an extended community list to configure Virtual Private Network (VPN) route filtering. Extended community attributes filter routes for virtual routing and forwarding instances (VRFs). The command uses regular expressions to name the communities specified by the list.</p> <ul style="list-style-type: none"> Route Target (rt) attribute identifies a set of sites and VRFs that may receive routes that are tagged with the configured route target. Configuring the route target extended attribute with a route allows that route to be placed in the per-site forwarding tables that route traffic received from corresponding sites. Site of Origin (soo) attribute uniquely identifies the site from which the provider edge (PE) router learned the route. All routes learned from a specific site must be assigned the same site of origin attribute whether a site is connected to a single PE router or multiple PE routers. Configuring this attribute prevents the creation of routing loops when a site is multihomed. The SOO extended community attribute is configured on the interface and is propagated into BGP through redistribution. The SOO should not be configured for stub sites or sites that are not multihomed. <p>The no ip extcommunity-list expanded and default ip extcommunity-list expanded commands delete the specified extended community list by removing the corresponding ip community-list expanded statement from <i>running-config</i>.</p> <p>Platform all Command Mode Global Configuration</p> <p>Command Syntax</p> <pre>ip extcommunity-list expanded listname FILTER_TYPE R_EXP no ip extcommunity-list expanded listname default ip extcommunity-list expanded listname</pre> <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1590.</p> <p>See also Arista User Manual v. 4.13.6F (4/14/2014), at 1540; Arista User Manual v. 4.12.3 (7/17/13), at 1364; Arista User Manual, v. 4.11.1 (1/11/13), at 1110; Arista User Manual v. 4.10.3 (10/22/12), at 922; Arista User Manual v. 4.9.3.2 (5/3/12), at 689; Arista User Manual v. 4.8.2 (11/18/11), at 519.</p>	<p>Dkt. 419-10 at PDF p. 177</p>

Cisco's Documentation	Arista's Documentation	Supporting Evidence In The Record
<p>ip extcommunity-list</p> <p>To create an extended community list to configure Virtual Private Network (VPN) route filtering, use the ip extcommunity-list command in global configuration mode. To delete the extended community list, use the no form of this command.</p> <p>Global Configuration Mode CLI</p> <pre>ip extcommunity-list expanded-list / expanded list-name {permit deny} [regular-expression] / standard-list / standard list-name {permit deny} [rt value] [soo value]</pre> <pre>no ip extcommunity-list expanded-list / expanded list-name / standard-list / standard list-name</pre> <p>To enter IP extended community-list configuration mode to create or configure an extended community-list, use the ip extcommunity-list command in global configuration mode. To delete the entire extended community list, use the no form of this command. To delete a single entry, use the no form in IP Extended community-list configuration mode.</p> <pre>ip extcommunity-list expanded-list / expanded list-name / standard-list / standard list-name</pre> <pre>no ip extcommunity-list expanded-list / expanded list-name / standard-list / standard list-name</pre> <p>Cisco IOS IP Routing Protocols Command Reference (June 10, 2005), at 116.</p>	<p>ip extcommunity-list expanded</p> <p>The ip extcommunity-list expanded command creates an extended community list to configure Virtual Private Network (VPN) route filtering. Extended community attributes filter routes for virtual routing and forwarding instances (VRFs). The command uses regular expressions to name the communities specified by the list.</p> <ul style="list-style-type: none"> Route Target (rt) attribute identifies a set of sites and VRFs that may receive routes that are tagged with the configured route target. Configuring the route target extended attribute with a route allows that route to be placed in the per-site forwarding tables that route traffic received from corresponding sites. Site of Origin (soo) attribute uniquely identifies the site from which the provider edge (PE) router learned the route. All routes learned from a specific site must be assigned the same site of origin attribute whether a site is connected to a single PE router or multiple PE routers. Configuring this attribute prevents the creation of routing loops when a site is multihomed. The SOO extended community attribute is configured on the interface and is propagated into BGP through redistribution. The SOO should not be configured for stub sites or sites that are not multihomed. <p>The no ip extcommunity-list expanded and default ip extcommunity-list expanded commands delete the specified extended community list by removing the corresponding ip community-list expanded statement from <i>running-config</i>.</p> <p>Platform all Command Mode Global Configuration</p> <p>Command Syntax</p> <pre>ip extcommunity-list expanded listname FILTER_TYPE R_EXP</pre> <pre>no ip extcommunity-list expanded listname</pre> <pre>default ip extcommunity-list expanded listname</pre> <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1590.</p> <p>See also Arista User Manual v. 4.13.6F (4/14/2014), at 1540; Arista User Manual v. 4.12.3 (7/17/13), at 1364; Arista User Manual, v. 4.11.1 (1/11/13), at 1110; Arista User Manual v. 4.10.3 (10/22/12), at 922; Arista User Manual v. 4.9.3.2 (5/3/12), at 689; Arista User Manual v. 4.8.2 (11/18/11), at 519.</p>	<p>Dkt. 419-10 at PDF p. 178</p>

Cisco's Documentation	Arista's Documentation	Supporting Evidence In The Record
<p>Route Target Extended Community Attribute</p> <p>The route target (RT) extended community attribute is configured with the <code>rt</code> keyword. This attribute is used to identify a set of sites and VRFs that may receive routes that are tagged with the configured route target. Configuring the route target extended attribute with a route allows that route to be placed in the per-site forwarding tables that are used for routing traffic that is received from corresponding sites.</p> <p>Site of Origin Extended Community Attribute</p> <p>The site of origin (SOO) extended community attribute is configured with the <code>soo</code> keyword. This attribute uniquely identifies the site from which the provider edge (PE) router learned the route. All routes learned from a particular site must be assigned the same site of origin extended community attribute, regardless if a site is connected to a single PE router or multiple PE routers. Configuring this attribute prevents routing loops from occurring when a site is multihomed. The SOO extended community attribute is configured on the interface and is propagated into BGP through redistribution. The SOO should not be configured for stub sites or sites that are not multihomed.</p> <p>Cisco IOS IP Routing: BGP Command Reference (2013), at 330.</p>	<p>ip extcommunity-list expanded</p> <p>The <code>ip extcommunity-list expanded</code> command creates an extended community list to configure Virtual Private Network (VPN) route filtering. Extended community attributes filter routes for virtual routing and forwarding instances (VRFs). The command uses regular expressions to name the communities specified by the list.</p> <ul style="list-style-type: none"> Route Target (<code>rt</code>) attribute identifies a set of sites and VRFs that may receive routes that are tagged with the configured route target. Configuring the route target extended attribute with a route allows that route to be placed in the per-site forwarding tables that route traffic received from corresponding sites. Site of Origin (<code>soo</code>) attribute uniquely identifies the site from which the provider edge (PE) router learned the route. All routes learned from a specific site must be assigned the same site of origin attribute whether a site is connected to a single PE router or multiple PE routers. Configuring this attribute prevents the creation of routing loops when a site is multihomed. The SOO extended community attribute is configured on the interface and is propagated into BGP through redistribution. The SOO should not be configured for stub sites or sites that are not multihomed. <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1590.</p> <p><i>See also</i> Arista User Manual v. 4.13.6F (4/14/2014), at 1540; Arista User Manual v. 4.12.3 (7/17/13), at 1364; Arista User Manual, v. 4.11.1 (1/11/13), at 1110; Arista User Manual v. 4.10.3 (10/22/12), at 922; Arista User Manual v. 4.9.3.2 (5/3/12), at 689; Arista User Manual v. 4.8.2 (11/18/11), at 519.</p>	<p>Dkt. 419-10 at PDF p. 179</p>

Cisco's Documentation	Arista's Documentation	Supporting Evidence In The Record
<p>Route Target Extended Community Attribute</p> <p>The route target (RT) extended community attribute is configured with the rt keyword. This attribute is used to identify a set of sites and VRFs that may receive routes that are tagged with the configured route target. Configuring the route target extended attribute with a route allows that route to be placed in the per-site forwarding tables that are used for routing traffic that is received from corresponding sites.</p> <p>Site of Origin Extended Community Attribute</p> <p>The site of origin (SOO) extended community attribute is configured with the soo keyword. This attribute uniquely identifies the site from which the provider edge (PE) router learned the route. All routes learned from a particular site must be assigned the same site of origin extended community attribute, regardless if a site is connected to a single PE router or multiple PE routers. Configuring this attribute prevents routing loops from occurring when a site is multihomed. The SOO extended community attribute is configured on the interface and is propagated into BGP through redistribution. The SOO should not be configured for stub sites or sites that are not multihomed.</p> <p>Cisco IOS IP Routing Protocols Command Reference (June 10, 2005), at 118.</p>	<p>ip extcommunity-list expanded</p> <p>The ip extcommunity-list expanded command creates an extended community list to configure Virtual Private Network (VPN) route filtering. Extended community attributes filter routes for virtual routing and forwarding instances (VRFs). The command uses regular expressions to name the communities specified by the list.</p> <ul style="list-style-type: none"> Route Target (rt) attribute identifies a set of sites and VRFs that may receive routes that are tagged with the configured route target. Configuring the route target extended attribute with a route allows that route to be placed in the per-site forwarding tables that route traffic received from corresponding sites. Site of Origin (soo) attribute uniquely identifies the site from which the provider edge (PE) router learned the route. All routes learned from a specific site must be assigned the same site of origin attribute whether a site is connected to a single PE router or multiple PE routers. Configuring this attribute prevents the creation of routing loops when a site is multihomed. The SOO extended community attribute is configured on the interface and is propagated into BGP through redistribution. The SOO should not be configured for stub sites or sites that are not multihomed. <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1590.</p> <p><i>See also</i> Arista User Manual v. 4.13.6F (4/14/2014), at 1540; Arista User Manual v. 4.12.3 (7/17/13), at 1364; Arista User Manual, v. 4.11.1 (1/11/13), at 1110; Arista User Manual v. 4.10.3 (10/22/12), at 922; Arista User Manual v. 4.9.3.2 (5/3/12), at 689; Arista User Manual v. 4.8.2 (11/18/11), at 519.</p>	<p>Dkt. 419-10 at PDF p. 180</p>

Cisco's Documentation	Arista's Documentation	Supporting Evidence In The Record
<p>Route Target Extended Community Attribute</p> <p>The route target (RT) extended community attribute is configured with the <code>rt</code> keyword. This attribute is used to identify a set of sites and VRFs that may receive routes that are tagged with the configured route target. Configuring the route target extended attribute with a route allows that route to be placed in the per-site forwarding tables that are used for routing traffic that is received from corresponding sites.</p> <p>Site of Origin Extended Community Attribute</p> <p>The site of origin (SOO) extended community attribute is configured with the <code>soo</code> keyword. This attribute uniquely identifies the site from which the provider edge (PE) router learned the route. All routes learned from a particular site must be assigned the same site of origin extended community attribute, regardless if a site is connected to a single PE router or multiple PE routers. Configuring this attribute prevents routing loops from occurring when a site is multihomed. The SOO extended community attribute is configured on the interface and is propagated into BGP through redistribution. The SOO should not be configured for stub sites or sites that are not multihomed.</p> <p>Cisco IOS IP Routing: BGP Command Reference (2013), at 330.</p>	<p>ip extcommunity-list standard</p> <p>The <code>ip extcommunity-list standard</code> command creates an extended community list to configure Virtual Private Network (VPN) route filtering. Extended community attributes filter routes for virtual routing and forwarding instances (VRFs).</p> <ul style="list-style-type: none"> Route Target (<code>rt</code>) attribute identifies a set of sites and VRFs that may receive routes that are tagged with the configured route target. Configuring the route target extended attribute with a route allows that route to be placed in the per-site forwarding tables that route traffic received from corresponding sites. Site of Origin (<code>soo</code>) attribute uniquely identifies the site from which the provider edge (PE) router learned the route. All routes learned from a specific site must be assigned the same site of origin attribute whether a site is connected to a single PE router or multiple PE routers. Configuring this attribute prevents the creation of routing loops when a site is multihomed. The SOO extended community attribute is configured on the interface and is propagated into BGP through redistribution. The SOO should not be configured for stub sites or sites that are not multihomed. <p>Arista User Manual v. 4.14.3F (Rev. 2) (October 2, 2014), at 1591.</p> <p>See also Arista User Manual v. 4.13.6F (4/14/2014), at 1541; Arista User Manual v. 4.12.3 (7/17/13), at 1365; Arista User Manual, v. 4.11.1 (1/11/13), at 1111; Arista User Manual v. 4.10.3 (10/22/12), at 923; Arista User Manual v. 4.9.3.2 (5/3/12), at 690; Arista User Manual v. 4.8.2 (11/18/11), at 520.</p>	<p>Dkt. 419-10 at PDF p. 181</p>

Cisco's Documentation	Arista's Documentation	Supporting Evidence In The Record
<p>Route Target Extended Community Attribute</p> <p>The route target (RT) extended community attribute is configured with the rt keyword. This attribute is used to identify a set of sites and VRFs that may receive routes that are tagged with the configured route target. Configuring the route target extended attribute with a route allows that route to be placed in the per-site forwarding tables that are used for routing traffic that is received from corresponding sites.</p> <p>Site of Origin Extended Community Attribute</p> <p>The site of origin (SOO) extended community attribute is configured with the soo keyword. This attribute uniquely identifies the site from which the provider edge (PE) router learned the route. All routes learned from a particular site must be assigned the same site of origin extended community attribute, regardless if a site is connected to a single PE router or multiple PE routers. Configuring this attribute prevents routing loops from occurring when a site is multihomed. The SOO extended community attribute is configured on the interface and is propagated into BGP through redistribution. The SOO should not be configured for stub sites or sites that are not multihomed.</p> <p>Cisco IOS IP Routing Protocols Command Reference (June 10, 2005), at 118.</p>	<p>ip extcommunity-list standard</p> <p>The ip extcommunity-list standard command creates an extended community list to configure Virtual Private Network (VPN) route filtering. Extended community attributes filter routes for virtual routing and forwarding instances (VRFs).</p> <ul style="list-style-type: none"> Route Target (rt) attribute identifies a set of sites and VRFs that may receive routes that are tagged with the configured route target. Configuring the route target extended attribute with a route allows that route to be placed in the per-site forwarding tables that route traffic received from corresponding sites. Site of Origin (soo) attribute uniquely identifies the site from which the provider edge (PE) router learned the route. All routes learned from a specific site must be assigned the same site of origin attribute whether a site is connected to a single PE router or multiple PE routers. Configuring this attribute prevents the creation of routing loops when a site is multihomed. The SOO extended community attribute is configured on the interface and is propagated into BGP through redistribution. The SOO should not be configured for stub sites or sites that are not multihomed. <p>Arista User Manual v. 4.14.3F (Rev. 2) (October 2, 2014), at 1591.</p> <p><i>See also</i> Arista User Manual v. 4.13.6F (4/14/2014), at 1541; Arista User Manual v. 4.12.3 (7/17/13), at 1365; Arista User Manual, v. 4.11.1 (1/11/13), at 1111; Arista User Manual v. 4.10.3 (10/22/12), at 923; Arista User Manual v. 4.9.3.2 (5/3/12), at 690; Arista User Manual v. 4.8.2 (11/18/11), at 520.</p>	<p>Dkt. 419-10 at PDF p. 182</p>

Cisco's Documentation	Arista's Documentation	Supporting Evidence In The Record
<p>Route Target Extended Community Attribute</p> <p>The route target (RT) extended community attribute is configured with the rt keyword. This attribute is used to identify a set of sites and VRFs that may receive routes that are tagged with the configured route target. Configuring the route target extended attribute with a route allows that route to be placed in the per-site forwarding tables that are used for routing traffic that is received from corresponding sites.</p> <p>Site of Origin Extended Community Attribute</p> <p>The site of origin (SOO) extended community attribute is configured with the soo keyword. This attribute uniquely identifies the site from which the provider edge (PE) router learned the route. All routes learned from a particular site must be assigned the same site of origin extended community attribute, regardless if a site is connected to a single PE router or multiple PE routers. Configuring this attribute prevents routing loops from occurring when a site is multihomed. The SOO extended community attribute is configured on the interface and is propagated into BGP through redistribution. The SOO should not be configured for stub sites or sites that are not multihomed.</p> <p>Cisco IOS IP Routing: BGP Command Reference (2013), at 330.</p>	<p>route targets (rt): This attribute identifies a set of sites and VRFs that may receive routes tagged with the configured route target. Configuring this attribute with a route allows that route to be placed in per-site forwarding tables that route traffic received from corresponding sites.</p> <p>site of origin (soo): This attribute identifies the site from where the Provider Edge (PE) router learns the route. All routes learned from a specific site have the same SOO extended community attribute, whether a site is connected to a single or multiple PE routers. This attribute prevents routing loops resulting from multihomed sites. The SOO attribute is configured on the interface and propagated into a BGP domain by redistribution. The SOO is applied to routes learned from VRFs.</p> <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1552.</p> <p><i>See also</i> Arista User Manual v. 4.13.6F (4/14/2014), at 1502; Arista User Manual v. 4.12.3 (7/17/13), at 1334; Arista User Manual, v. 4.11.1 (1/11/13), at 1083-84; Arista User Manual v. 4.10.3 (10/22/12), at 896; Arista User Manual v. 4.9.3.2 (5/3/12), at 668; Arista User Manual v. 4.8.2 (11/18/11), at 500.</p>	Dkt. 419-10 at PDF p. 183
<p>Route Target Extended Community Attribute</p> <p>The route target (RT) extended community attribute is configured with the rt keyword. This attribute is used to identify a set of sites and VRFs that may receive routes that are tagged with the configured route target. Configuring the route target extended attribute with a route allows that route to be placed in the per-site forwarding tables that are used for routing traffic that is received from corresponding sites.</p> <p>Site of Origin Extended Community Attribute</p> <p>The site of origin (SOO) extended community attribute is configured with the soo keyword. This attribute uniquely identifies the site from which the provider edge (PE) router learned the route. All routes learned from a particular site must be assigned the same site of origin extended community attribute, regardless if a site is connected to a single PE router or multiple PE routers. Configuring this attribute prevents routing loops from occurring when a site is multihomed. The SOO extended community attribute is configured on the interface and is propagated into BGP through redistribution. The SOO should not be configured for stub sites or sites that are not multihomed.</p> <p>Cisco IOS IP Routing Protocols Command Reference (June 10, 2005), at 118.</p>	<p>route targets (rt): This attribute identifies a set of sites and VRFs that may receive routes tagged with the configured route target. Configuring this attribute with a route allows that route to be placed in per-site forwarding tables that route traffic received from corresponding sites.</p> <p>site of origin (soo): This attribute identifies the site from where the Provider Edge (PE) router learns the route. All routes learned from a specific site have the same SOO extended community attribute, whether a site is connected to a single or multiple PE routers. This attribute prevents routing loops resulting from multihomed sites. The SOO attribute is configured on the interface and propagated into a BGP domain by redistribution. The SOO is applied to routes learned from VRFs.</p> <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1552.</p> <p><i>See also</i> Arista User Manual v. 4.13.6F (4/14/2014), at 1502; Arista User Manual v. 4.12.3 (7/17/13), at 1334; Arista User Manual, v. 4.11.1 (1/11/13), at 1083-84; Arista User Manual v. 4.10.3 (10/22/12), at 896; Arista User Manual v. 4.9.3.2 (5/3/12), at 668; Arista User Manual v. 4.8.2 (11/18/11), at 500.</p>	Dkt. 419-10 at PDF p. 183

Cisco's Documentation	Arista's Documentation	Supporting Evidence In The Record
<p>Extended community attributes are used to configure, filter, and identify routes for virtual routing and forwarding instances (VRFs) and Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs).</p> <p>Cisco IOS IP Routing: BGP Command Reference (2013), at 359</p>	<p>BGP extended communities configure, filter, and identify routes for virtual routing, forwarding instances (VRFs), and Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs).</p> <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/22014), at 1552.</p> <p>See also Arista User Manual v. 4.13.6F (4/14/2014), at 1502; Arista User Manual v. 4.12.3 (7/17/13), at 1334; Arista User Manual, v. 4.11.1 (1/11/13), at 1083-84; Arista User Manual v. 4.10.3 (10/22/12), at 896; Arista User Manual v. 4.9.3.2 (5/3/12), at 668; Arista User Manual v. 4.8.2 (11/18/11), at 500.</p>	<p>Dkt. 419-10 at PDF p. 184</p>
<p>Extended community attributes are used to configure, filter, and identify routes for virtual routing and forwarding instances (VRFs) and Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs).</p> <p>Cisco IOS IP Routing Protocols Command Reference (June 10, 2005), at 135.</p>	<p>BGP extended communities configure, filter, and identify routes for virtual routing, forwarding instances (VRFs), and Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs).</p> <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/22014), at 1552.</p> <p>See also Arista User Manual v. 4.13.6F (4/14/2014), at 1502; Arista User Manual v. 4.12.3 (7/17/13), at 1334; Arista User Manual, v. 4.11.1 (1/11/13), at 1083-84; Arista User Manual v. 4.10.3 (10/22/12), at 896; Arista User Manual v. 4.9.3.2 (5/3/12), at 668; Arista User Manual v. 4.8.2 (11/18/11), at 500.</p>	<p>Dkt. 419-10 at PDF p. 184</p>

Cisco's Documentation	Arista's Documentation	Supporting Evidence In The Record
<p>neighbor ebgp-multihop</p> <p>To accept and attempt BGP connections to external peers residing on networks that are not directly connected, use the neighbor ebgp-multihop command in router configuration mode. To return to the default, use the no form of this command.</p> <p>neighbor {ip-address ipv6-address peer-group-name} ebgp-multihop [ttl]</p> <p>no neighbor {ip-address ipv6-address peer-group-name} ebgp-multihop</p> <p>Cisco IOS IP Routing: BGP Command Reference (2013), at 423.</p>	<p>neighbor ebgp-multihop</p> <p>The neighbor ebgp-multihop command programs the switch to accept and attempt BGP connections to the external peers residing on networks not directly connected to the switch. The command does not establish the multihop if the only route to the peer is the default route (0.0.0.0).</p> <p>The no neighbor ebgp-multihop command applies the system default configuration.</p> <p>The default neighbor ebgp-multihop command applies the system default configuration for individual neighbors, and applies the peer group's setting for neighbors that are members of a peer group.</p> <p>The no neighbor command removes all configuration commands for the neighbor at the specified address.</p> <p>Platform all Command Mode Router-BGP Configuration</p> <p>Command Syntax</p> <p>neighbor NEIGHBOR_ID ebgp-multihop [hop_number] no neighbor NEIGHBOR_ID ebgp-multihop default neighbor NEIGHBOR_ID ebgp-multihop</p> <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1597.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1370; Arista User Manual, v. 4.11.1 (1/11/13), at 1116; Arista User Manual v. 4.10.3 (10/22/12), at 928; Arista User Manual v. 4.9.3.2 (5/3/12), at 693; Arista User Manual v. 4.8.2 (11/18/11), at 523; Arista User Manual v. 4.7.3 (7/18/11), at 383.</p>	<p>Dkt. 419-10 at PDF p. 185</p>

Cisco's Documentation	Arista's Documentation	Supporting Evidence In The Record
<p>neighbor ebgp-multihop</p> <p>To accept and attempt Border Gateway Protocol (BGP) connections to external peers residing on networks that are not directly connected, use the neighbor ebgp-multihop command in router configuration mode. To return to the default, use the no form of this command.</p> <p>neighbor ip-address peer-group-name ebgp-multihop [ttl]</p> <p>no neighbor ip-address peer-group-name ebgp-multihop</p> <p>Cisco IOS IP Routing Protocols Command Reference (June 10, 2005), at 158.</p>	<p>neighbor ebgp-multihop</p> <p>The neighbor ebgp-multihop command programs the switch to accept and attempt BGP connections to the external peers residing on networks not directly connected to the switch. The command does not establish the multihop if the only route to the peer is the default route (0.0.0.0).</p> <p>The no neighbor ebgp-multihop command applies the system default configuration.</p> <p>The default neighbor ebgp-multihop command applies the system default configuration for individual neighbors, and applies the peer group's setting for neighbors that are members of a peer group.</p> <p>The no neighbor command removes all configuration commands for the neighbor at the specified address.</p> <p>Platform all Command Mode Router-BGP Configuration</p> <p>Command Syntax</p> <p>neighbor NEIGHBOR_ID ebgp-multihop [hop_number] no neighbor NEIGHBOR_ID ebgp-multihop default neighbor NEIGHBOR_ID ebgp-multihop</p> <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1597.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1370; Arista User Manual, v. 4.11.1 (1/11/13), at 1116; Arista User Manual v. 4.10.3 (10/22/12), at 928; Arista User Manual v. 4.9.3.2 (5/3/12), at 693; Arista User Manual v. 4.8.2 (11/18/11), at 523; Arista User Manual v. 4.7.3 (7/18/11), at 383.</p>	<p>Dkt. 419-10 at PDF p. 186</p>

Cisco’s Documentation	Arista’s Documentation	Supporting Evidence In The Record						
<div>neighbor local-as</div> <div>To customize the AS_PATH attribute for routes received from an external Border Gateway Protocol (eBGP) neighbor, or to configure the BGP—Support for iBGP Local-AS feature, use the neighbor local-as command in address family or router configuration mode. To disable AS_PATH attribute customization or iBGP Local-AS support, use the no form of this command.</div> <div>neighbor {ip-address ipv6-address peer-group-name} local-as [autonomous-system-number [no-prepend [replace-as [dual-as]]]]</div> <div>no neighbor {ip-address ipv6-address peer-group-name} local-as</div> <div>...</div> <div><table><tr><td>no-prepend</td><td>(Optional) Does not prepend the local autonomous system number to any routes received from the eBGP neighbor.</td></tr></table></div>	no-prepend	(Optional) Does not prepend the local autonomous system number to any routes received from the eBGP neighbor.	<div>neighbor local-as</div> <div>The neighbor local-as command enables the modification of the AS_PATH attribute for routes received from an eBGP neighbor, allowing the switch to appear as a member of a different autonomous system (AS) to external peers. This switch does not prepend the local AS number to routes received from the eBGP neighbor. The AS number from the local BGP routing process is not prepended.</div> <div>The no neighbor local-as command disables AS_PATH modification for the specified peer or peer group.</div> <div>The default neighbor local-as command disables AS_PATH modification for individual neighbors, and applies the peer group’s setting for neighbors that are members of a peer group.</div> <div><table><tr><td>Platform</td><td>all</td></tr><tr><td>Command Mode</td><td>Router-BGP Configuration</td></tr></table></div> <div>Command Syntax</div> <div>neighbor NEIGHBOR_ID local-as as_id no-prepend replace-as</div> <div>no neighbor NEIGHBOR_ID local-as</div> <div>default neighbor NEIGHBOR_ID local-as</div>	Platform	all	Command Mode	Router-BGP Configuration	Dkt. 419-10 at PDF p. 187
no-prepend	(Optional) Does not prepend the local autonomous system number to any routes received from the eBGP neighbor.							
Platform	all							
Command Mode	Router-BGP Configuration							
Cisco IOS IP Routing: BGP Command Reference (2013), at 442.	Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1601.							
	See also Arista User Manual v. 4.12.3 (7/17/13), at 1373; Arista User Manual, v. 4.11.1 (1/11/13), at 1119; Arista User Manual v. 4.10.3 (10/22/12), at 931; Arista User Manual v. 4.9.3.2 (5/3/12), at 696; Arista User Manual v. 4.8.2 (11/18/11), at 526; Arista User Manual v. 4.7.3 (7/18/11), at 386.							

Cisco's Documentation	Arista's Documentation	Supporting Evidence In The Record
<p>neighbor local-as</p> <p>To customize the AS-path attribute for routes received from an external Border Gateway Protocol (eBGP) neighbor, use the neighbor local-as command in address family or router configuration mode. To disable AS-path attribute customization, use the no form of this command.</p> <p>neighbor <i>ip-address</i> local-as <i>as-number</i> [<i>no-prepend</i> [<i>replace-as</i> [<i>dual-as</i>]]]</p> <p>no neighbor <i>ip-address</i> local-as <i>as-number</i></p> <p>...</p> <p>no-prepend (Optional) Does not prepend the local autonomous system number to any routes received from the eBGP neighbor.</p> <p>Cisco IOS IP Routing Protocols Command Reference (June 10, 2005), at 166.</p>	<p>neighbor local-as</p> <p>The neighbor local-as command enables the modification of the AS_PATH attribute for routes received from an eBGP neighbor, allowing the switch to appear as a member of a different autonomous system (AS) to external peers. This switch does not prepend the local AS number to routes received from the eBGP neighbor. The AS number from the local BGP routing process is not prepended.</p> <p>The no neighbor local-as command disables AS_PATH modification for the specified peer or peer group.</p> <p>The default neighbor local-as command disables AS_PATH modification for individual neighbors, and applies the peer group's setting for neighbors that are members of a peer group.</p> <p>Platform all Command Mode Router-BGP Configuration</p> <p>Command Syntax</p> <p>neighbor <i>NEIGHBOR_ID</i> local-as <i>as_id</i> [no-prepend [replace-as [no neighbor <i>NEIGHBOR_ID</i> local-as]]]</p> <p>default neighbor <i>NEIGHBOR_ID</i> local-as</p> <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1601.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1373; Arista User Manual, v. 4.11.1 (1/11/13), at 1119; Arista User Manual v. 4.10.3 (10/22/12), at 931; Arista User Manual v. 4.9.3.2 (5/3/12), at 696; Arista User Manual v. 4.8.2 (11/18/11), at 526; Arista User Manual v. 4.7.3 (7/18/11), at 386.</p>	<p>Dkt. 419-10 at PDF p. 188</p>

Cisco's Documentation

neighbor remove-private-as

To remove private autonomous system numbers from the autonomous system path (a list of autonomous systems that a route passes through to reach a BGP peer) in eBGP outbound routing updates, use the **neighbor remove-private-as** command in router configuration, address family configuration, or peer-group template mode. To disable this function, use the **no** form of this command.

neighbor {*ip-address* | *peer-group-name*} **remove-private-as** [**all** [**replace-as**]]

no neighbor {*ip-address* | *peer-group-name*} **remove-private-as**

Syntax Description

<i>ip-address</i>	IP address of the BGP-speaking neighbor.
<i>peer-group-name</i>	Name of a BGP peer group.
all	(Optional) Removes all private AS numbers from the AS path in outgoing updates.
replace-as	(Optional) As long as the all keyword is specified, the replace-as keyword causes all private AS numbers in the AS path to be replaced with the router's local AS number.

Cisco IOS IP Routing: BGP Command Reference (2013), at 479.

Arista's Documentation

neighbor remove-private-as

The **neighbor remove-private-as** command removes private autonomous system numbers from outbound routing updates for external BGP (eBGP) neighbors. When the autonomous system path includes both private and public autonomous system numbers, the **REMOVAL** parameter specifies how the private autonomous system number is removed.

The **no neighbor remove-private-as** command applies the system default (preserves private AS numbers) for the specified peer.

The default **neighbor remove-private-as** command applies the system default for individual neighbors, and applies the peer group's setting for neighbors that are members of a peer group.

The **no neighbor** command removes all configuration commands for the neighbor at the specified address.

Platform all
Command Mode Router-BGP Configuration

Command Syntax

neighbor *NEIGHBOR_ID* **remove-private-as** [**REMOVAL**]
no neighbor *NEIGHBOR_ID* **remove-private-as**
default neighbor *NEIGHBOR_ID* **remove-private-as**

Parameters

- NEIGHBOR_ID** IP address or peer group name. Values include:
 - ipv4_addr* neighbor's IPv4 address.
 - ipv6_addr* neighbor's IPv6 address.
 - group_name* peer group name.
- REMOVAL** Specifies removal of private autonomous AS number when path includes both private and public numbers. Values include:
 - <no parameter>** private AS numbers are not removed.
 - all** removes all private AS numbers from AS path in outbound updates.
 - all replace-as** all private AS numbers in AS path are replaced with router's local AS number.

Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1612.

See also Arista User Manual v. 4.12.3 (7/17/13), at 1384; Arista User Manual, v. 4.11.1 (1/11/13), at 1130.

Supporting Evidence In The Record

Dkt. 419-10 at PDF p. 189

Cisco's Documentation	Arista's Documentation	Supporting Evidence In The Record
<p>neighbor remove-private-as</p> <p>To remove private autonomous system numbers from the autonomous system path, a list of autonomous system numbers that a route passes through to reach a BGP peer, in outbound routing updates, use the neighbor remove-private-as command in router configuration mode. To disable this function, use the no form of this command.</p> <pre>neighbor {ip-address peer-group-name} remove-private-as no neighbor {ip-address peer-group-name} remove-private-as</pre> <p>Cisco IOS IP Routing Protocols Command Reference (June 10, 2005), at 188.</p>	<p>neighbor remove-private-as</p> <p>The neighbor remove-private-as command removes private autonomous system numbers from outbound routing updates for external BGP (eBGP) neighbors. When the autonomous system path includes both private and public autonomous system numbers, the <i>REMOVAL</i> parameter specifies how the private autonomous system number is removed.</p> <p>The no neighbor remove-private-as command applies the system default (preserves private AS numbers) for the specified peer.</p> <p>The default neighbor remove-private-as command applies the system default for individual neighbors, and applies the peer group's setting for neighbors that are members of a peer group.</p> <p>The no neighbor command removes all configuration commands for the neighbor at the specified address.</p> <p>Platform all Command Mode Router-BGP Configuration</p> <p>Command Syntax</p> <pre>neighbor NEIGHBOR_ID remove-private-as [REMOVAL] no neighbor NEIGHBOR_ID remove-private-as default neighbor NEIGHBOR_ID remove-private-as</pre> <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1612.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 1384; Arista User Manual, v. 4.11.1 (1/11/13), at 1130.</p>	<p>Dkt. 419-10 at PDF p. 190</p>

Cisco's Documentation	Arista's Documentation	Supporting Evidence In The Record				
<div>neighbor route-reflector-client</div> <p>To configure the router as a BGP route reflector and configure the specified neighbor as its client, use the neighbor route-reflector-client command in address family or router configuration mode. To indicate that the neighbor is not a client, use the no form of this command.</p> <div>neighbor {ip-address ipv6-address peer-group-name} route-reflector-client</div> <div>no neighbor {ip-address ipv6-address peer-group-name} route-reflector-client</div> <p>Cisco IOS IP Routing: BGP Command Reference (2013), at 486</p> <p>By default, all internal BGP (iBGP) speakers in an autonomous system must be fully meshed, and neighbors do not readvertise iBGP learned routes to neighbors, thus preventing a routing information loop. When all the clients are disabled, the local router is no longer a route reflector.</p> <p>If you use route reflectors, all iBGP speakers need not be fully meshed. In the route reflector model, an Internal BGP peer is configured to be a <i>route reflector</i> responsible for passing iBGP learned routes to iBGP neighbors. This scheme eliminates the need for each router to talk to every other router.</p> <div>Use the neighbor route-reflector-client command to configure the local router as the route reflector and the specified neighbor as one of its clients. All the neighbors configured with this command will be members of the client group and the remaining iBGP peers will be members of the nonclient group for the local route reflector.</div> <div>The bgp client-to-client reflection command controls client-to-client reflection.</div> <p>Cisco IOS IP Routing: BGP Command Reference (2013), at 487.</p>	<div>neighbor route-reflector-client</div> <p>Participating BGP routers within an AS communicate EBGP-learned routes to all of their peers, but to prevent routing loops they must not re-advertise iBGP-learned routes within the AS. To ensure that all members of the AS share the same routing information, a fully meshed network topology (in which each member router of the AS is connected to every other member) can be used, but this topology can result in high volumes of iBGP messages when it is scaled. Instead, in larger networks one or more routers can be configured as route reflectors.</p> <p>A route reflector is configured to re-advertise routes learned through iBGP to a group of BGP neighbors within the AS (its clients), eliminating the need for a fully meshed topology.</p> <div>The neighbor route-reflector-client command configures the switch to act as a route reflector and configures the specified neighbor as one of its clients. Additional clients can be specified by re-issuing the command.</div> <div>The bgp client-to-client reflection command controls client-to-client reflection.</div> <p>The no neighbor route-reflector-client and default neighbor route-reflector-client commands disable route reflection by deleting the neighbor route-reflector-client command from <i>running-config</i>.</p> <table><tr><td>Platform</td><td>all</td></tr><tr><td>Command Mode</td><td>Router-BGP Configuration</td></tr></table> <p>Command Syntax</p> <div>neighbor NEIGHBOR_ID route-reflector-client</div> <div>no neighbor NEIGHBOR_ID route-reflector-client</div> <div>default neighbor NEIGHBOR_ID route-reflector-client</div> <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1614.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1386; Arista User Manual, v. 4.11.1 (1/11/13), at 1132.</p>	Platform	all	Command Mode	Router-BGP Configuration	Dkt. 419-10 at PDF p. 191
Platform	all					
Command Mode	Router-BGP Configuration					

Cisco's Documentation	Arista's Documentation	Supporting Evidence In The Record
<p>neighbor route-reflector-client</p> <p>To configure the router as a BGP route reflector and configure the specified neighbor as its client, use the neighbor route-reflector-client command in address family or router configuration mode. To indicate that the neighbor is not a client, use the no form of this command.</p> <p>neighbor <i>ip-address</i> route-reflector-client</p> <p>no neighbor <i>ip-address</i> route-reflector-client</p> <p>Usage Guidelines</p> <p>By default, all internal BGP (iBGP) speakers in an autonomous system must be fully meshed, and neighbors do not readvertise iBGP learned routes to neighbors, thus preventing a routing information loop. When all the clients are disabled, the local router is no longer a route reflector.</p> <p>If you use route reflectors, all iBGP speakers need not be fully meshed. In the route reflector model, an Interior BGP peer is configured to be a <i>route reflector</i> responsible for passing iBGP learned routes to iBGP neighbors. This scheme eliminates the need for each router to talk to every other router.</p> <p>Use the neighbor route-reflector-client command to configure the local router as the route reflector and the specified neighbor as one of its clients. All the neighbors configured with this command will be members of the client group and the remaining iBGP peers will be members of the nonclient group for the local route reflector.</p> <p>The bgp client-to-client reflection command controls client-to-client reflection.</p> <p>Cisco IOS IP Routing Protocols Command Reference (June 10, 2005), at 192.</p>	<p>neighbor route-reflector-client</p> <p>Participating BGP routers within an AS communicate EBGP-learned routes to all of their peers, but to prevent routing loops they must not re-advertise iBGP-learned routes within the AS. To ensure that all members of the AS share the same routing information, a fully meshed network topology (in which each member router of the AS is connected to every other member) can be used, but this topology can result in high volumes of iBGP messages when it is scaled. Instead, in larger networks one or more routers can be configured as route reflectors.</p> <p>A route reflector is configured to re-advertise routes learned through iBGP to a group of BGP neighbors within the AS (its clients), eliminating the need for a fully meshed topology.</p> <p>The neighbor route-reflector-client command configures the switch to act as a route reflector and configures the specified neighbor as one of its clients. Additional clients can be specified by re-issuing the command.</p> <p>The bgp client-to-client reflection command controls client-to-client reflection.</p> <p>The no neighbor route-reflector-client and default neighbor route-reflector-client commands disable route reflection by deleting the neighbor route-reflector-client command from <i>running-config</i>.</p> <p>Platform all</p> <p>Command Mode Router-BGP Configuration</p> <p>Command Syntax</p> <p>neighbor <i>NEIGHBOR_ID</i> route-reflector-client</p> <p>no neighbor <i>NEIGHBOR_ID</i> route-reflector-client</p> <p>default neighbor <i>NEIGHBOR_ID</i> route-reflector-client</p> <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1614.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1386; Arista User Manual, v. 4.11.1 (1/11/13), at 1132.</p>	<p>Dkt. 419-10 at PDF p. 192</p>

Cisco's Documentation		Arista's Documentation	Supporting Evidence In The Record
neighbor ebgp-multihop	Accepts and attempts BGP connections to external peers residing on networks that are not directly connected.	<p>neighbor ebgp-multihop</p> <p>The neighbor ebgp-multihop command programs the switch to accept and attempt BGP connections to the external peers residing on networks not directly connected to the switch. The command does not establish the multihop if the only route to the peer is the default route (0.0.0.0).</p> <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1597.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1370; Arista User Manual, v. 4.11.1 (1/11/13), at 1116; Arista User Manual v. 4.10.3 (10/22/12), at 928; Arista User Manual v. 4.9.3.2 (5/3/12), at 693; Arista User Manual v. 4.8.2 (11/18/11), at 523; Arista User Manual v. 4.7.3 (7/18/11), at 383.</p>	Dkt. 419-10 at PDF p. 193
neighbor ebgp-multihop	Accepts and attempts BGP connections to external peers residing on networks that are not directly connected.	<p>neighbor ebgp-multihop</p> <p>The neighbor ebgp-multihop command programs the switch to accept and attempt BGP connections to the external peers residing on networks not directly connected to the switch. The command does not establish the multihop if the only route to the peer is the default route (0.0.0.0).</p> <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1597.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1370; Arista User Manual, v. 4.11.1 (1/11/13), at 1116; Arista User Manual v. 4.10.3 (10/22/12), at 928; Arista User Manual v. 4.9.3.2 (5/3/12), at 693; Arista User Manual v. 4.8.2 (11/18/11), at 523; Arista User Manual v. 4.7.3 (7/18/11), at 383.</p>	Dkt. 419-10 at PDF p. 193

Cisco's Documentation	Arista's Documentation	Supporting Evidence In The Record
<div data-bbox="69 293 873 339"> <div>neighbor route-map</div> <div>Applies a route map to inbound or outbound routes.</div> </div> <p>Cisco IOS IP Routing: BGP Command Reference (2013), at 524.</p>	<p>neighbor route-map (BGP)</p> <p>The neighbor route-map command applies a route map to inbound or outbound BGP routes. When a route map is applied to outbound routes, the switch will advertise only routes matching at least one section of the route map. Only one outbound route map and one inbound route map can be applied to a given neighbor. A new route map applied to a neighbor will replace the previous route map.</p> <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1613.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1385; Arista User Manual, v. 4.11.1 (1/11/13), at 1131; Arista User Manual v. 4.10.3 (10/22/12), at 943.</p>	Dkt. 419-10 at PDF p. 194
<div data-bbox="69 678 892 708"> <div>neighbor route-map</div> <div>Applies a route map to inbound or outbound routes.</div> </div> <p>Cisco IOS IP Routing Protocols Command Reference (June 10, 2005), at 204.</p>	<p>neighbor route-map (BGP)</p> <p>The neighbor route-map command applies a route map to inbound or outbound BGP routes. When a route map is applied to outbound routes, the switch will advertise only routes matching at least one section of the route map. Only one outbound route map and one inbound route map can be applied to a given neighbor. A new route map applied to a neighbor will replace the previous route map.</p> <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1613.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1385; Arista User Manual, v. 4.11.1 (1/11/13), at 1131; Arista User Manual v. 4.10.3 (10/22/12), at 943.</p>	Dkt. 419-10 at PDF p. 194

Cisco's Documentation

show ip bgp ipv4 multicast summary

To display a summary of IP Version 4 multicast database-related information, use the `show ip bgp ipv4 multicast summary` command in EXEC mode.

`show ip bgp ipv4 multicast summary`

Cisco IOS IP Routing: BGP Command Reference (2013), at 757

Table 54: show ip bgp ipv4 multicast summary Field Descriptions

Field	Description
Neighbor	IP address of configured neighbor in the multicast routing table.
V	Version of multiprotocol BGP used.
AS	Autonomous system to which the neighbor belongs.
MsgRcvd	Number of messages received from the neighbor.
MsgSent	Number of messages sent to the neighbor.
TblVer	Number of the table version, which is incremented each time the table changes.
InQ	Number of messages received in the input queue.
OutQ	Number of messages ready to go in the output queue.
Up/Down	Days and hours that the neighbor has been up or down (no information in the State column means the connection is up).
State/PfxRcd	State of the neighbor/number of routes received. If no state is indicated, the state is up.

Cisco IOS IP Routing: BGP Command Reference (2013), at 758.

Arista's Documentation

show ip bgp summary

The `show ip bgp summary` command displays BGP path, prefix, and attribute information for all BGP neighbors.

Platform all
Command Mode EXEC

Command Syntax

`show ip bgp summary` [VRF_INSTANCE]

Parameters

- `VRF_INSTANCE` specifies VRF instances.
 - <no parameter> displays routing table for context-active VRF.
 - `vrf vrf_name` displays routing table for the specified VRF.
 - `vrf all` displays routing table for all VRFs.
 - `vrf default` displays routing table for default VRF.

Display Values

Header Row

- BGP router identifier: The router identifier – loopback address or highest IP address.
- Local AS Number: AS number assigned to switch

Neighbor Table Columns

- (First) Neighbor: IP address of the neighbor.
- (Second) V: BGP version number spoken to the neighbor
- (Third) AS: Neighbor's Autonomous system number.
- (Fourth) MsgRcvd: Number of messages received from the neighbor.
- (Fifth) MsgSent: Number of messages sent to the neighbor.
- (Sixth) InQ: Number of messages queued to be processed from the neighbor.
- (Seventh) OutQ: Number of messages queued to be sent to the neighbor.
- (Eighth) Up/Down: Period the BGP session has been in Established state or its current status.
- (Ninth) State: State of the BGP session and the number of routes received from a neighbor.

Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1641.

See also Arista User Manual v. 4.12.3 (7/17/13), at 1407; Arista User Manual, v. 4.11.1 (1/11/13), at 1153; Arista User Manual v. 4.10.3 (10/22/12), at 964; Arista User Manual v. 4.9.3.2 (5/3/12), at 728; Arista User Manual v. 4.8.2 (11/18/11), at 549; Arista User Manual v. 4.7.3 (7/18/11), at 402.

Supporting Evidence In The Record

Dkt. 419-10 at PDF p. 195

Cisco's Documentation

show ip bgp ipv4 multicast summary

To display a summary of IP Version 4 multicast database-related information, use the **show ip bgp ipv4 multicast summary** command in EXEC mode.

show ip bgp ipv4 multicast summary

Table 27 *show ip bgp ipv4 multicast summary Field Descriptions*

Field	Description
Neighbor	IP address of configured neighbor in the multicast routing table.
V	Version of multiprotocol BGP used.
AS	Autonomous system to which the neighbor belongs.
MsgRcvd	Number of messages received from the neighbor.
MsgSent	Number of messages sent to the neighbor.
TblVer	Number of the table version, which is incremented each time the table changes.
InQ	Number of messages received in the input queue.
OutQ	Number of messages ready to go in the output queue.
Up/Down	Days and hours that the neighbor has been up or down (no information in the State column means the connection is up).
State/PfxRcd	State of the neighbor/number of routes received. If no state is indicated, the state is up.

Cisco IOS IP Routing Protocols Command Reference (June 10, 2005), at 308.

Arista's Documentation

show ip bgp summary

The **show ip bgp summary** command displays BGP path, prefix, and attribute information for all BGP neighbors.

Platform all
Command Mode EXEC

Command Syntax

show ip bgp summary [*VRF_INSTANCE*]

Parameters

- *VRF_INSTANCE* specifies VRF instances.
 - <no parameter> displays routing table for context-active VRF.
 - *vrf vrf_name* displays routing table for the specified VRF.
 - *vrf all* displays routing table for all VRFs.
 - *vrf default* displays routing table for default VRF.

Display Values

Header Row

- BGP router identifier: The router identifier – loopback address or highest IP address.
- Local AS Number: AS number assigned to switch

Neighbor Table Columns

- (First) **Neighbor**: IP address of the neighbor.
- (Second) **V**: BGP version number spoken to the neighbor
- (Third) **AS**: Neighbor's Autonomous system number.
- (Fourth) **MsgRcvd**: Number of messages received from the neighbor.
- (Fifth) **MsgSent**: Number of messages sent to the neighbor.
- (Sixth) **InQ**: Number of messages queued to be processed from the neighbor.
- (Seventh) **OutQ**: Number of messages queued to be sent to the neighbor.
- (Eighth) **Up/Down**: Period the BGP session has been in Established state or its current status.
- (Ninth) **State**: State of the BGP session and the number of routes received from a neighbor.

Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1641.

See also Arista User Manual v. 4.12.3 (7/17/13), at 1407; Arista User Manual, v. 4.11.1 (1/11/13), at 1153; Arista User Manual v. 4.10.3 (10/22/12), at 964; Arista User Manual v. 4.9.3.2 (5/3/12), at 728; Arista User Manual v. 4.8.2 (11/18/11), at 549; Arista User Manual v. 4.7.3 (7/18/11), at 402.

Supporting Evidence In The Record

Dkt. 419-10 at PDF p. 196

Cisco's Documentation

The following is sample output from the `show ip bgp paths` command in privileged EXEC mode:

```
Router# show ip bgp paths
Address      Hash Refcount Metric Path
0x60E5742C   0       1       0 1
0x60E3D7AC   2       1       0 ?
0x60E5C6C0  11       3       0 10 ?
0x60E577B0  35       2      40 10 ?
```

The table below describes the significant fields shown in the display.

Table 64: show ip bgp paths Field Descriptions

Field	Description
Address	Internal address where the path is stored.
Hash	Hash bucket where path is stored.
Refcount	Number of routes using that path.
Metric	The Multi Exit Discriminator (MED) metric for the path. (The name of this metric for BGP versions 2 and 3 is INTER_AS.)
Path	The autonomous system path for that route, followed by the origin code for that route.

Cisco IOS IP Routing: BGP Command Reference (2013), at 795.

Arista's Documentation

show ip bgp paths

The show ip bgp paths command displays all BGP paths in the database.

Platform all
Command Mode EXEC

Command Syntax

`show ip bgp paths [VRF_INSTANCE]`

Parameters

- `VRF_INSTANCE` specifies VRF instances.
 - `<no parameter>` displays routing table for context-active VRF.
 - `vrf vrf_name` displays routing table for the specified VRF.
 - `vrf all` displays routing table for all VRFs.
 - `vrf default` displays routing table for default VRF.

Display Values

- `Refcount`: Number of routes using a listed path.
- `Metric`: The Multi Exit Discriminator (MED) metric for the path.
- `Path`: The autonomous system path for that route, followed by the origin code for that route.

Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1638,

See also Arista User Manual v. 4.13.6F (4/14/2014), at 1588; Arista User Manual v. 4.12.3 (7/17/13), at 1405; Arista User Manual, v. 4.11.1 (1/11/13), at 1151; Arista User Manual v. 4.10.3 (10/22/12), at 962; Arista User Manual v. 4.9.3.2 (5/3/12), at 725; Arista User Manual v. 4.8.2 at 547; Arista User Manual v. 4.8.2 (11/18/11), at 547; Arista User Manual v. 4.7.3 (7/18/11), at 401; Arista User Manual v. 4.6.0 (12/22/2010), at 249; Arista User Manual v. 4.6.0 (12/22/2010), at 249

Supporting Evidence In The Record

Dkt. 419-10 at PDF p. 197

Cisco's Documentation

The following is sample output from the `show ip bgp paths` command in privileged EXEC mode:

Router# `show ip bgp paths`

```
Address      Hash Refcount Metric Path
0x60B5742C   0         1      0 i
0x60B3D7AC   2         1      0 ?
0x60B5C6C0  11         3      0 10 ?
0x60B577B0  35         2     40 10 ?
```

Table 33 describes the significant fields shown in the display.

Table 33 *show ip bgp paths* Field Descriptions

Field	Description
Address	Internal address where the path is stored.
Hash	Hash bucket where path is stored.
Refcount	Number of routes using that path.
Metric	The Multi Exit Discriminator (MED) metric for the path. (The name of this metric for BGP versions 2 and 3 is INTER_AS.)
Path	The autonomous system path for that route, followed by the origin code for that route.

Cisco IOS IP Routing Protocols Command Reference (June 10, 2005), at 308.

Arista's Documentation

`show ip bgp paths`

The `show ip bgp paths` command displays all BGP paths in the database.

Platform all
Command Mode EXEC

Command Syntax

`show ip bgp paths [VRF_INSTANCE]`

Parameters

- `VRF_INSTANCE` specifies VRF instances.
 - `<no parameter>` displays routing table for context-active VRF.
 - `vrf vrf_name` displays routing table for the specified VRF.
 - `vrf all` displays routing table for all VRFs.
 - `vrf default` displays routing table for default VRF.

Display Values

- Refcount: Number of routes using a listed path.
- Metric: The Multi Exit Discriminator (MED) metric for the path.
- Path: The autonomous system path for that route, followed by the origin code for that route.

Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1638,

See also Arista User Manual v. 4.13.6F (4/14/2014), at 1588; Arista User Manual v. 4.12.3 (7/17/13), at 1405; Arista User Manual, v. 4.11.1 (1/11/13), at 1151; Arista User Manual v. 4.10.3 (10/22/12), at 962; Arista User Manual v. 4.9.3.2 (5/3/12), at 725; Arista User Manual v. 4.8.2 at 547; Arista User Manual v. 4.8.2 (11/18/11), at 547; Arista User Manual v. 4.7.3 (7/18/11), at 401; Arista User Manual v. 4.6.0 (12/22/2010), at 249; Arista User Manual v. 4.6.0 (12/22/2010), at 249

Supporting Evidence In The Record

Dkt. 419-10 at PDF p. 198

Cisco's Documentation	Arista's Documentation	Supporting Evidence In The Record
<p data-bbox="71 293 873 337">The show ip bgp summary command is used to display BGP path, prefix, and attribute information for all connections to BGP neighbors.</p> <p data-bbox="58 378 823 407">Cisco IOS IP Routing: BGP Command Reference (2013), at 819.</p>	<p data-bbox="940 289 1234 318">show ip bgp summary</p> <p data-bbox="940 342 1814 386">The show ip bgp summary command displays BGP path, prefix, and attribute information for all BGP neighbors.</p> <p data-bbox="930 431 1644 461">Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1641.</p> <p data-bbox="930 496 1780 659"><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 1407; Arista User Manual, v. 4.11.1 (1/11/13), at 1153; Arista User Manual v. 4.10.3 (10/22/12), at 964; Arista User Manual v. 4.9.3.2 (5/3/12), at 728; Arista User Manual v. 4.8.2 (11/18/11), at 549; Arista User Manual v. 4.7.3 (7/18/11), at 402.</p>	<p data-bbox="1850 289 2024 350">Dkt. 419-10 at PDF p. 199</p>
<p data-bbox="71 708 894 751">The show ip bgp summary command is used to display BGP path, prefix, and attribute information for all connections to BGP neighbors.</p> <p data-bbox="58 800 884 862">Cisco IOS IP Routing Protocols Command Reference (July 16, 2005), at 323.</p>	<p data-bbox="940 699 1234 729">show ip bgp summary</p> <p data-bbox="940 753 1814 797">The show ip bgp summary command displays BGP path, prefix, and attribute information for all BGP neighbors.</p> <p data-bbox="930 842 1644 872">Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1641.</p> <p data-bbox="930 907 1780 1070"><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 1407; Arista User Manual, v. 4.11.1 (1/11/13), at 1153; Arista User Manual v. 4.10.3 (10/22/12), at 964; Arista User Manual v. 4.9.3.2 (5/3/12), at 728; Arista User Manual v. 4.8.2 (11/18/11), at 549; Arista User Manual v. 4.7.3 (7/18/11), at 402.</p>	<p data-bbox="1850 699 2024 761">Dkt. 419-10 at PDF p. 199</p>

Cisco's Documentation	Arista's Documentation	Supporting Evidence In The Record				
<table><tr><td>Up/Down</td><td>The length of time that the BGP session has been in the Established state, or the current status if not in the Established state.</td></tr></table> <p>Cisco IOS IP Routing: BGP Command Reference (2013), at 821.</p> <table><tr><td>State/PfxRcd</td><td><p>Current state of the BGP session, and the number of prefixes that have been received from a neighbor or peer group. When the maximum number (as set by the neighbor maximum-prefix command) is reached, the string "PfxRcd" appears in the entry, the neighbor is shut down, and the connection is set to Idle.</p><p>An (Admin) entry with Idle status indicates that the connection has been shut down using the neighbor shutdown command.</p></td></tr></table> <p>Cisco IOS IP Routing: BGP Command Reference (2013), at 822.</p>	Up/Down	The length of time that the BGP session has been in the Established state, or the current status if not in the Established state.	State/PfxRcd	<p>Current state of the BGP session, and the number of prefixes that have been received from a neighbor or peer group. When the maximum number (as set by the neighbor maximum-prefix command) is reached, the string "PfxRcd" appears in the entry, the neighbor is shut down, and the connection is set to Idle.</p> <p>An (Admin) entry with Idle status indicates that the connection has been shut down using the neighbor shutdown command.</p>	<p>Neighbor Table Columns</p> <ul style="list-style-type: none">• (First) Neighbor: IP address of the neighbor.• (Second) V: BGP version number spoken to the neighbor• (Third) AS: Neighbor's Autonomous system number.• (Fourth) MsgRcvd: Number of messages received from the neighbor.• (Fifth) MsgSent: Number of messages sent to the neighbor.• (Sixth) InQ: Number of messages queued to be processed from the neighbor.• (Seventh) OutQ: Number of messages queued to be sent to the neighbor.• (Eighth) Up/Down: Period the BGP session has been in Established state or its current status.• (Ninth) State: State of the BGP session and the number of routes received from a neighbor. <p>After the maximum number of routes are received (maximum paths (BGP)), the field displays PfxRcd, the neighbor is shut down, and the connection is set to Idle.</p> <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1641.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1407; Arista User Manual, v. 4.11.1 (1/11/13), at 1153; Arista User Manual v. 4.10.3 (10/22/12), at 964; Arista User Manual v. 4.9.3.2 (5/3/12), at 728.</p>	Dkt. 419-10 at PDF p. 200
Up/Down	The length of time that the BGP session has been in the Established state, or the current status if not in the Established state.					
State/PfxRcd	<p>Current state of the BGP session, and the number of prefixes that have been received from a neighbor or peer group. When the maximum number (as set by the neighbor maximum-prefix command) is reached, the string "PfxRcd" appears in the entry, the neighbor is shut down, and the connection is set to Idle.</p> <p>An (Admin) entry with Idle status indicates that the connection has been shut down using the neighbor shutdown command.</p>					
<table><tr><td>Up/Down</td><td>The length of time that the BGP session has been in the Established state, or the current state if it is not Established.</td></tr><tr><td>State/PfxRcd</td><td><p>Current state of the BGP session/the number of prefixes the router has received from a neighbor or peer group. When the maximum number (as set by the neighbor maximum-prefix command) is reached, the string "PfxRcd" appears in the entry, the neighbor is shut down, and the connection is Idle.</p><p>An (Admin) entry with Idle status indicates that the connection has been shut down using the neighbor shutdown command.</p></td></tr></table> <p>Cisco IOS IP Routing Protocols Command Reference (June 10, 2005), at 318.</p>	Up/Down	The length of time that the BGP session has been in the Established state, or the current state if it is not Established.	State/PfxRcd	<p>Current state of the BGP session/the number of prefixes the router has received from a neighbor or peer group. When the maximum number (as set by the neighbor maximum-prefix command) is reached, the string "PfxRcd" appears in the entry, the neighbor is shut down, and the connection is Idle.</p> <p>An (Admin) entry with Idle status indicates that the connection has been shut down using the neighbor shutdown command.</p>	<p>Neighbor Table Columns</p> <ul style="list-style-type: none">• (First) Neighbor: IP address of the neighbor.• (Second) V: BGP version number spoken to the neighbor• (Third) AS: Neighbor's Autonomous system number.• (Fourth) MsgRcvd: Number of messages received from the neighbor.• (Fifth) MsgSent: Number of messages sent to the neighbor.• (Sixth) InQ: Number of messages queued to be processed from the neighbor.• (Seventh) OutQ: Number of messages queued to be sent to the neighbor.• (Eighth) Up/Down: Period the BGP session has been in Established state or its current status.• (Ninth) State: State of the BGP session and the number of routes received from a neighbor. <p>After the maximum number of routes are received (maximum paths (BGP)), the field displays PfxRcd, the neighbor is shut down, and the connection is set to Idle.</p> <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1641.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1407; Arista User Manual, v. 4.11.1 (1/11/13), at 1153; Arista User Manual v. 4.10.3 (10/22/12), at 964; Arista User Manual v. 4.9.3.2 (5/3/12), at 728.</p>	Dkt. 419-10 at PDF p. 200
Up/Down	The length of time that the BGP session has been in the Established state, or the current state if it is not Established.					
State/PfxRcd	<p>Current state of the BGP session/the number of prefixes the router has received from a neighbor or peer group. When the maximum number (as set by the neighbor maximum-prefix command) is reached, the string "PfxRcd" appears in the entry, the neighbor is shut down, and the connection is Idle.</p> <p>An (Admin) entry with Idle status indicates that the connection has been shut down using the neighbor shutdown command.</p>					

Cisco's Documentation

bfd

To set the baseline Bidirectional Forwarding Detection (BFD) session parameters on an interface, use the `bfd` command in interface configuration mode. To remove the baseline BFD session parameters, use the `no` form of this command.

```
bfd interval milliseconds min_rx milliseconds multiplier multiplier-value
no bfd interval milliseconds min_rx milliseconds multiplier multiplier-value
```

Syntax Description

<code>interval milliseconds</code>	Specifies the rate, in milliseconds, at which BFD control packets will be sent to BFD peers. The valid range for the <code>milliseconds</code> argument is from 50 to 999.
<code>min_rx milliseconds</code>	Specifies the rate, in milliseconds, at which BFD control packets will be expected to be received from BFD peers. The valid range for the <code>milliseconds</code> argument is from 50 to 999.
<code>multiplier multiplier-value</code>	Specifies the number of consecutive BFD control packets that must be missed from a BFD peer before BFD declares that the peer is unavailable and the Layer 3 BFD peer is informed of the failure. The valid range for the <code>multiplier-value</code> argument is from 3 to 50.

Cisco IOS IP Routing: Protocol-Independent Command Reference (2013), at 9

Arista's Documentation

bfd

The `bfd` command configures BFD parameters for the configuration mode interface. All BFD sessions that pass through this interface will use these parameters. If custom parameters are not configured, the interface will use default values for BFD sessions passing through it.

For a BFD session to be established, BFD must be enabled for any routing protocol using BFD for failure detection.

The `no bfd` and `default bfd` commands return the BFD parameters on the configuration mode interface to default values by removing the corresponding `bfd` command from *running-config*.

Platform	all
Command Mode	Interface-Ethernet Configuration Interface-Loopback Configuration Interface-Management Configuration Interface-Port-channel Configuration Interface-VLAN Configuration

Command Syntax

```
bfd interval transmit_rate min_rx receive_minimum multiplier factor
no bfd
default bfd
```

Parameters

- `transmit_rate` specifies the rate in milliseconds at which BFD control packets will be sent to BFD peers. Values range from 50 to 60000; the default value is 300.
- `receive_minimum` specifies the rate in milliseconds at which BFD control packets will be expected from BFD peers. Values range from 50 to 60000.
- `factor` specifies the number of consecutive missed BFD control packets from a BFD peer that will designate the peer as unavailable and indicate failure to the Layer 3 BFD peer. Values range from 3 to 50.

Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1741.

See also Arista User Manual v. 4.12.3 (7/17/13), at 1471.

Supporting Evidence In The Record

Dkt. 419-10 at PDF p. 201

Cisco's Documentation	Arista's Documentation	Supporting Evidence In The Record
<p>ip route</p> <p>To establish static routes, use the <code>ip route</code> command in global configuration mode. To remove static routes, use the <code>no ip route</code> command.</p> <p><code>ip route</code> [vrf vrf-name] prefix mask {ip-address} interface-type interface-number [ip-address] [dhcp] [global] [distance] [multicast] [name next-hop-name] [permanent] [track number] [tag tag]</p> <p><code>no ip route</code> [vrf vrf-name] prefix mask {ip-address} interface-type interface-number [ip-address] [dhcp] [global] [distance] [multicast] [name next-hop-name] [permanent] [track number] [tag tag]</p> <p>Cisco IOS IP Routing: Protocol-Independent Command Reference (2013), at 62</p> <p>If you specify an administrative distance, you are flagging a static route that can be overridden by dynamic information. For example, routes derived with Enhanced Interior Gateway Routing Protocol (EIGRP) have a default administrative distance of 100. To have a static route that would be overridden by an EIGRP dynamic route, specify an administrative distance greater than 100. Static routes have a default administrative distance of 1.</p> <p>Cisco IOS IP Routing: Protocol-Independent Command Reference (2013), at 63</p>	<p>ip route</p> <p>The <code>ip route</code> command creates a static route. The destination is a network segment; the next-hop address is either an IPv4 address or a routable port. When multiple routes exist to a destination prefix, the route with the lowest administrative distance takes precedence.</p> <p>Static routes have a default administrative distance of 1. Assigning a higher administrative distance to a static route configures it to be overridden by dynamic routing data. For example, a static route with a distance value of 200 is overridden by OSPF intra-area routes with a default distance of 110.</p> <p>...</p> <p>Command Syntax</p> <p><code>ip route</code> [VRF_INSTANCE] dest_net NEXTHOP [DISTANCE] [TAG_OPTION] [RT_NAME]</p> <p><code>no ip route</code> [VRF_INSTANCE] dest_net [NEXTHOP] [DISTANCE]</p> <p><code>default ip route</code> [VRF_INSTANCE] dest_net [NEXTHOP] [DISTANCE]</p> <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1287.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1082; Arista User Manual, v. 4.11.1 (1/11/13), at 860; Arista User Manual v. 4.10.3 (10/22/12), at 683.</p>	Dkt. 419-10 at PDF p. 202
<p>show ipv6 route summary</p> <p>Displays the current contents of the IPv6 routing table in summary format.</p> <p>Cisco IOS IP Routing: Protocol-Independent Command Reference (2013), at 284</p>	<p>show ipv6 route summary</p> <p>The <code>show ipv6 route summary</code> command displays the current contents of the IPv6 routing table in summary format.</p> <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1337.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1165.</p>	Dkt. 419-10 at PDF p. 202

Cisco's Documentation	Arista's Documentation	Supporting Evidence In The Record
<p>Usage Guidelines Learn lists are a way to categorize learned traffic classes. In each learn list, different criteria for learning traffic classes including prefixes, application definitions, filters, and aggregation parameters can be configured. A traffic class is automatically learned by PIR based on each learn list criteria, and each learn list is configured with a sequence number. <u>The sequence number determines the order in which</u> learn list criteria are applied. Learn lists allow different PIR policies to be applied to each learn list; in previous releases the traffic classes could not be divided, and a PIR policy was applied to all the traffic classes profiled during one learning session.</p> <p>Cisco IOS Performance Routing Command Reference (2010), at 131.</p>	<p>Route maps define conditions for redistributing routes between routing protocols. A route map clause is identified by a name, filter type (permit or deny) and sequence number. <u>Clauses with the same name are components of a single route map; the sequence number determines the order in which</u> the clauses are compared to a route.</p> <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 894.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 773; Arista User Manual, v. 4.11.1 (1/11/13), at 602; Arista User Manual v. 4.10.3 (10/22/12), at 516; Arista User Manual v. 4.9.3.2 (5/3/12), at 439; Arista User Manual v. 4.8.2 (11/18/11), at 316.</p>	<p>Dkt. 419-10 at PDF p. 203</p>
<p>Usage Guidelines The <code>set interface</code> command is entered on a master controller in PIR map configuration mode. This command can be used for PIR black hole filtering if the border routers detect a denial-of-service (DoS) attack by directing packets to the null interface. <u>The null interface is a virtual network interface that</u> is similar to the loopback interface. Whereas traffic to the loopback interface is directed to the router itself, traffic sent to the null interface is discarded. This interface is always up and can never forward or receive traffic; encapsulation always fails. The null interface functions similarly to the null devices available on most operating systems. Null interfaces are used as a low-overhead method of discarding unnecessary network traffic.</p> <p>Cisco IOS Performance Routing Command Reference (2010), at 226.</p>	<p>14.4.6 Null0 Interface</p> <p><u>The null0 interface is a virtual interface that</u> drops all inbound packets. A null0 route is a network route whose destination is <i>null0 interface</i>. Inbound packets to a null0 interface are not forwarded to any valid address. Many interface configuration commands provide <i>null0</i> as an interface option.</p> <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 633.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 502; Arista User Manual, v. 4.11.1 (1/11/13), at 397; Arista User Manual v. 4.10.3 (10/22/12), at 329.</p>	<p>Dkt. 419-10 at PDF p. 203</p>

Cisco's Documentation	Arista's Documentation	Supporting Evidence In The Record						
<div>snmp-server enable traps pfr</div> <div>To enable Performance Routing (PFR) Simple Network Management Protocol (SNMP) notifications (traps and informs), use the snmp-server enable traps pfr command in global configuration mode. To disable PFR notifications, use the no form of this command.</div> <div>snmp-server enable traps pfr</div> <div>no snmp-server enable traps pfr</div> <div><div>Syntax Description</div><div>This command has no arguments or keywords.</div></div> <div><div>Command Default</div><div>PFR SNMP notifications are disabled.</div></div> <div><div>Command Modes</div><div>Global configuration (config)</div></div> <div><div>Command History</div><table><thead><tr><th>Release</th><th>Modification</th></tr></thead><tbody><tr><td>Cisco IOS XE Release 3.7S</td><td>This command was introduced.</td></tr><tr><td>15.3(2)T</td><td>This command was integrated into Cisco IOS Release 15.3(2)T.</td></tr></tbody></table></div> <div><div>Usage Guidelines</div><div>Use this command to enable SNMP notifications for PFR activity.</div></div> <div><div>Examples</div><div>This example shows how to enable PFR SNMP notifications:</div><div>Router(config)# snmp-server host 10.2.2.2 traps public pfr Router(config)# snmp-server enable traps pfr Router(config)# exit</div></div>	Release	Modification	Cisco IOS XE Release 3.7S	This command was introduced.	15.3(2)T	This command was integrated into Cisco IOS Release 15.3(2)T.	<div>snmp-server enable traps</div> <div>The snmp-server enable traps command enables the transmission of Simple Network Management Protocol (SNMP) notifications as traps or inform requests. This command enables both traps and inform requests for the specified notification types. The snmp-server host command specifies the notification type (traps or informs). Sending notifications requires at least one snmp-server host command.</div> <div>The snmp-server enable traps and no snmp-server enable traps commands, without an MIB parameter, specifies the default notification trap generation setting for all MIBs. These commands, when specifying an MIB, controls notification generation for the specified MIB. The default snmp-server enable traps command resets notification generation to the default setting for the specified MIB.</div> <div><div>Platform</div><div>all</div></div> <div><div>Command Mode</div><div>Global Configuration</div></div> <div><div>Command Syntax</div><div>snmp-server enable traps [trap_type] no snmp-server enable traps [trap_type] default snmp-server enable traps [trap_type]</div></div> <div><div>Parameters</div><div><ul style="list-style-type: none">trap_type controls the generation of informs or traps for the specified MIB:<ul style="list-style-type: none"><no parameter> controls notifications for MIBs not covered by specific commands.entity controls entity-MIB modification notifications.lldp controls LLDP notifications.msdpBackwardTransition controls msdpBackwardTransition notifications.msdpEstablished controls msdpEstablished notifications.snmp controls SNMP-v2 notifications.switchover controls switchover notifications.snmpConfigManEvent controls snmpConfigManEvent notifications.test controls test traps.</div></div> <div><div>Examples</div><div><ul style="list-style-type: none">These commands enables notification generation for all MIBs except spanning tree.<div>switch(config)#snmp-server enable traps switch(config)#no snmp-server enable traps spanning-tree switch(config)#</div>This command enables spanning-tree MIB notification generation, regardless of the default setting.<div>switch(config)#snmp-server enable traps spanning-tree switch(config)#</div></div></div>	Dkt. 419-10 at PDF pp. 204-205
Release	Modification							
Cisco IOS XE Release 3.7S	This command was introduced.							
15.3(2)T	This command was integrated into Cisco IOS Release 15.3(2)T.							

Cisco IOS Performance Routing Command Reference (2010), at 372.

Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1990.

See also Arista User Manual v. 4.12.3 (7/17/13), at 1680; Arista User Manual, v. 4.11.1 (1/11/13), at 1365; Arista User Manual v. 4.10.3

Cisco’s Documentation	Arista’s Documentation	Supporting Evidence In The Record				
	(10/22/12), at 1132; Arista User Manual v. 4.9.3.2 (5/3/12), at 888; Arista User Manual v. 4.8.2 (11/18/11), at 696; Arista User Manual v. 4.7.3 (7/18/11), at 552.					
<div><div>no snmp-server</div><div>To disable Simple Network Management Protocol (SNMP) agent operation, use the no snmp-server command in global configuration mode.</div><div>no snmp-server</div><div><div>Syntax Description</div><div>This command has no arguments or keywords.</div></div><div><div>Command Default</div><div>No default behavior or values.</div></div><div><div>Command Modes</div><div>Global configuration</div></div><div><div>Command History</div><table><thead><tr><th>Release</th><th>Modification</th></tr></thead><tbody><tr><td>10.0</td><td>This command was introduced.</td></tr></tbody></table></div><div><div>Usage Guidelines</div><div>This command disables all running versions of SNMP (SNMPv1, SNMPv2C, and SNMPv3) on the device.</div></div><div><div>Examples</div><div>The following example disables the current running version of SNMP:</div><div>Router(config)# no snmp-server</div></div></div> <div>Cisco IOS SNMP Support Command Reference (2013), at 52.</div>	Release	Modification	10.0	This command was introduced.	<div><div>no snmp-server</div><div>The no snmp-server and default snmp-server commands disable Simple Network Management Protocol (SNMP) agent operation by removing all snmp-server commands from running-config. SNMP is enabled with any snmp-server community or snmp-server user command.</div><div><div>Platform</div><div>all</div></div><div><div>Command Mode</div><div>Global Configuration</div></div><div><div>Command Syntax</div><div>no snmp-server</div><div>default snmp-server</div></div><div><div>Example</div><div><ul style="list-style-type: none">This command disables SNMP agent operation on the switch<div>switch(config)#no snmp-server</div><div>switch(config)#</div></div></div><div>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1973.</div><div>See also Arista User Manual v. 4.12.3 (7/17/13), at 1663; Arista User Manual, v. 4.11.1 (1/11/13), at 1350; Arista User Manual v. 4.10.3 (10/22/12), at 1117; Arista User Manual v. 4.9.3.2 (5/3/12), at 873; Arista User Manual v. 4.8.2 (11/18/11), at 681; Arista User Manual v. 4.7.3 (7/18/11), at 537.</div></div>	Dkt. 419-10 at PDF p. 205
Release	Modification					
10.0	This command was introduced.					

Cisco's Documentation	Arista's Documentation	Supporting Evidence In The Record
<p>Examples</p> <p>The following is sample output from the <code>show snmp</code> command:</p> <pre> Router# show snmp Chassis: 12161083 0 SNMP packets input 0 Bad SNMP version errors 0 Unknown community name 0 Illegal operation for community name supplied 0 Encoding errors 0 Number of requested variables 0 Number of altered variables 0 Get-request PDUs 0 Get-next PDUs 0 Set-request PDUs 0 Input queue packet drops (Maximum queue size 1000) 0 SNMP packets output 0 Too big errors (Maximum packet size 1500) 0 No such name errors 0 Bad values errors 0 General errors 0 Response PDUs 0 Trap PDUs SNMP logging: enabled SNMP trap Queue: 0 dropped due to resource failure. </pre> <p>Cisco IOS SNMP Support Command Reference (2013), at 83.</p>	<p>Example</p> <ul style="list-style-type: none"> This command configures <code>xyz-1234</code> as the chassis-ID string, then displays the result. <pre> switch(config)#snmp-server chassis-id xyz-1234 switch(config)#show snmp Chassis: xyz-1234 <---chassis ID 8 SNMP packets input 0 Bad SNMP version errors 0 Unknown community name 0 Illegal operation for community name supplied 0 Encoding errors 8 Number of requested variables 0 Number of altered variables 4 Get-request PDUs 4 Get-next PDUs 0 Set-request PDUs 21 SNMP packets output 0 Too big errors 0 No such name errors 0 Bad value errors 0 General errors 8 Response PDUs 0 Trap PDUs SNMP logging: enabled Logging to taccon.162 SNMP agent enabled switch(config)# </pre> <p>Arista User Manual v. 4.14.3F (Rev. 2) (October 2, 2014), at 1967-68.</p> <p>See also Arista User Manual v. 4.13.6F (4/14/2014), at 1896; Arista User Manual v. 4.12.3 (7/17/13), at 1658; Arista User Manual, v. 4.11.1 (1/11/13), at 1344-45; Arista User Manual v. 4.10.3 (10/22/12), at 1111; Arista User Manual v. 4.9.3.2 (5/3/12), at 867; Arista User Manual v. 4.8.2 (11/18/11), at 678; Arista User Manual v. 4.7.3 (7/18/11), at 534.</p>	<p>Dkt. 419-10 at PDF p. 206</p>

Cisco's Documentation	Arista's Documentation	Supporting Evidence In The Record								
<div><div>show snmp engineID</div><div>To display the identification of the local Simple Network Management Protocol (SNMP) engine and all remote engines that have been configured on the router, use the show snmp engineID command in EXEC mode.</div><div>show snmp engineID</div><div><div>Syntax Description</div><div>This command has no arguments or keywords.</div></div><div><div>Command Modes</div><div>EXEC</div></div><div><div>Command History</div><table><tr><th>Release</th><th>Modification</th></tr><tr><td>12.0(3)T</td><td>This command was introduced.</td></tr><tr><td>12.2(33)SRA</td><td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td></tr><tr><td>12.2SX</td><td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td></tr></table></div><div><div>Usage Guidelines</div><div>An SNMP engine is a copy of SNMP that can reside on a local or remote device.</div></div><div><div>Examples</div><div><div>The following example specifies 0000000902000000C025808 as the local engineID and 123456789ABCDEF0000000000 as the remote engine ID, 172.16.37.61 as the IP address of the remote engine (copy of SNMP) and 162 as the port from which the remote device is connected to the local device:</div><div>Router# show snmp engineID Local SNMP engineID: 0000000902000000C025808 Remote Engine ID IP-addr Port 123456789ABCDEF0000000000 172.16.37.61 162</div><div>The table below describes the fields shown in the display.</div></div></div><div>Cisco IOS SNMP Support Command Reference (2013), at 91.</div></div>	Release	Modification	12.0(3)T	This command was introduced.	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.	<div><div>show snmp engineID</div><div>The show snmp engineID command displays the identification of the local Simple Network Management Protocol (SNMP) engine and of all remote engines that are configured on the switch.</div><div><div>Platformall</div><div>Command ModeEXEC</div></div><div><div>Command Syntax</div><div>show snmp engineID</div></div><div><div>Example</div><div><div>This command displays the ID of the local SNMP engine.</div><div>switch>show snmp engineid Local SNMP EngineID: f5717f001c730436d700 switch></div></div></div><div>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1978.</div><div>See also Arista User Manual v. 4.12.3 (7/17/13), at 1668; Arista User Manual, v. 4.11.1 (1/11/13), at 1355; Arista User Manual v. 4.10.3 (10/22/12), at 1122; Arista User Manual v. 4.9.3.2 (5/3/12), at 878; Arista User Manual v. 4.8.2 (11/18/11), at 686; Arista User Manual v. 4.7.3 (7/18/11), at 542.</div></div>	Dkt. 419-10 at PDF p. 207
Release	Modification									
12.0(3)T	This command was introduced.									
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.									
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.									

Cisco's Documentation	Arista's Documentation	Supporting Evidence In The Record				
<div>Related Commands</div> <table><thead><tr><th>Command</th><th>Description</th></tr></thead><tbody><tr><td>snmp-server engineID local</td><td>Configures a name for either the local or remote SNMP engine on the router.</td></tr></tbody></table> <p>Cisco IOS SNMP Support Command Reference (2013), at 92.</p>	Command	Description	snmp-server engineID local	Configures a name for either the local or remote SNMP engine on the router.	<div>Configuring the Engine ID</div> <p>The snmp-server engineID remote command configures the name for the local or remote Simple Network Management Protocol (SNMP) engine. An SNMP engine ID is a name for the local or remote SNMP engine.</p> <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1966.</p> <p>See also Arista User Manual v. 4.13.6F (4/14/2014), at 1894; Arista User Manual v. 4.12.3 (7/17/13), at 1656; Arista User Manual, v. 4.11.1 (1/11/13), at 1343; Arista User Manual v. 4.10.3 (10/22/12), at 1109; Arista User Manual v. 4.9.3.2 (5/3/12), at 865; Arista User Manual v. 4.8.2 (11/18/11), at 676; Arista User Manual v. 4.7.3 (7/18/11), at 432.</p>	Dkt. 419-10 at PDF p. 208
Command	Description					
snmp-server engineID local	Configures a name for either the local or remote SNMP engine on the router.					
<table><tr><td>security model</td><td>The security model used by the group, either v1, v2c, or v3.</td></tr></table> <p>Cisco IOS SNMP Support Command Reference (2013), at 92.</p>	security model	The security model used by the group, either v1, v2c, or v3.	<div><ul style="list-style-type: none">• VERSION the security model used by the group.<ul style="list-style-type: none">— v1 SNMPv1. Uses a community string match for authentication.— v2c SNMPv2c. Uses a community string match for authentication.— v3 no auth SNMPv3. Uses a username match for authentication.— v3 auth SNMPv3. HMAC-MD5 or HMAC-SHA authentication.— v3 priv SNMPv3. HMAC-MD5 or HMAC-SHA authentication. AES or DES encryption.</div> <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1994.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1684; Arista User Manual, v. 4.11.1 (1/11/13), at 1369; Arista User Manual v. 4.10.3 (10/22/12), at 1136; Arista User Manual v. 4.9.3.2 (5/3/12), at 892; Arista User Manual v. 4.8.2 (11/18/11), at 699; Arista User Manual v. 4.7.3 (7/18/11), at 555.</p>	Dkt. 419-10 at PDF p. 208		
security model	The security model used by the group, either v1, v2c, or v3.					

Cisco's Documentation

show snmp host

To display the recipient details for Simple Network Management Protocol (SNMP) notification operations, use the **show snmp host** command in privileged EXEC mode.

show snmp host

Syntax Description This command has no arguments or keywords.

Command Default The information configured for SNMP notification operation is displayed.

Command Modes Privileged EXEC (#)

Release	Modification
12.4(12)T	This command was introduced.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2SX	This command was integrated into Cisco IOS Release 12.2SX.

Usage Guidelines The **show snmp host** command displays details such as IP address of the Network Management System (NMS), notification type, SNMP version, and the port number of the NMS. To configure these details, use the **snmp-server host** command.

Examples The following is sample output from the **show snmp host** command.

```
Router# show snmp host
Notification host: 10.2.28.6 udp-port: 162 type: inform
user: public security model: v2c
traps: 00000000.00000000.00000000
```

The table below describes the significant fields shown in the display.

Table 5: show snmp host Field Descriptions

Field	Description
Notification host	Displays the IP address of the host for which the notification is generated.
udp-port	Displays the port number.
type	Displays the type of notification.
Field	Description
user	Displays the access type of the user for which the notification is generated.
security model	Displays the SNMP version used to send notifications.
traps	Displays details of the notification generated.

Related Commands	Command	Description
	snmp-server host	Configures the recipient details for SNMP notification operations.

Cisco IOS SNMP Support Command Reference (2013), at 95-96.

Arista's Documentation

show snmp host

The **show snmp host** command displays the recipient details for Simple Network Management Protocol (SNMP) notification operations. Details that the command displays include IP address and port number of the Network Management System (NMS), notification type, and SNMP version.

Platform all
Command Mode EXEC

Command Syntax

show snmp host

Field Descriptions

- **Notification host** IP address of the host for which the notification is generated.
- **udp-port** port number.
- **type** notification type.
- **user** access type of the user for which the notification is generated.
- **security model** SNMP version used to send notifications.
- **traps** details of the notification generated.

Example

- This command displays the hosts configured on the switch.

```
switch# show snmp host
Notification host: 172.22.22.20 udp-port: 162 type: trap
user: public security model: v2c

switch>
```

Arista User Manual v.4.14.3F (Rev. 2) (10/2/2014), at 1980.

See also Arista User Manual v. 4.13.6F (4/14/2014), at 1908; Arista User Manual v. 4.12.3 (7/17/13), at 1670; Arista User Manual, v. 4.11.1 (1/11/13), at 1357; Arista User Manual v. 4.10.3 (10/22/12), at 1124; Arista User Manual v. 4.9.3.2 (5/3/12), at 880; Arista User Manual v. 4.8.2 (11/18/11), at 688; Arista User Manual v. 4.7.3 (7/18/11), at 544.

Supporting Evidence In The Record

Dkt. 419-10 at PDF p. 209

Cisco's Documentation	Arista's Documentation	Supporting Evidence In The Record								
<div><div>show snmp location</div><div>To display the Simple Network Management Protocol (SNMP) system location string, use the show snmp locationcommand in privileged EXEC mode.</div><div>show snmp location</div><div><div>Syntax Description</div><div>This command has no arguments or keywords.</div></div><div><div>Command Default</div><div>The SNMP system location information is displayed.</div></div><div><div>Command Modes</div><div>Privileged EXEC (#)</div></div><div><div>Command History</div><table><thead><tr><th>Release</th><th>Modification</th></tr></thead><tbody><tr><td>12.4(12)T</td><td>This command was introduced.</td></tr><tr><td>12.2(31)SB</td><td>This command was integrated into Cisco IOS Release 12.2(31)SB2.</td></tr><tr><td>12.2SX</td><td>This command was integrated into Cisco IOS Release 12.2SX.</td></tr></tbody></table></div><div><div>Usage Guidelines</div><div>To configure system location details, use the snmp-server locationcommand.</div></div></div> <div>Cisco IOS SNMP Support Command Reference (2013), at 97.</div>	Release	Modification	12.4(12)T	This command was introduced.	12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB2.	12.2SX	This command was integrated into Cisco IOS Release 12.2SX.	<div><div>show snmp location</div><div>The show snmp location command displays the Simple Network Management Protocol (SNMP) system location string. The snmp-server location command configures system location details. The command has no effect if a location string was not previously configured.</div><div><div>Platform</div><div>all</div></div><div><div>Command Mode</div><div>EXEC</div></div><div><div>Command Syntax</div><div>show snmp location</div></div></div> <div>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1980.</div> <div>See also Arista User Manual v. 4.12.3 (7/17/13), at 1671; Arista User Manual, v. 4.11.1 (1/11/13), at 1358; Arista User Manual v. 4.10.3 (10/22/12), at 1125; Arista User Manual v. 4.9.3.2 (5/3/12), at 881; Arista User Manual v. 4.8.2 (11/18/11), at 689; Arista User Manual v. 4.7.3 (7/18/11), at 545.</div>	Dkt. 419-10 at PDF p. 210
Release	Modification									
12.4(12)T	This command was introduced.									
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB2.									
12.2SX	This command was integrated into Cisco IOS Release 12.2SX.									
<div>SNMP management information is viewed as a collection of managed objects, residing in a virtual information store, termed the Management Information Base (MIB). Collections of related objects are defined in MIB modules. These modules are written using a subset of OSI's Abstract Syntax Notation One (ASN.1), termed the Structure of Management Information (SMI).</div> <div>Cisco IOS SNMP Support Command Reference (2013), at 98..</div>	<div><div>Management Information Base (MIB):</div><div>The MIB stores network management information, which consists of collections of managed objects. Within the MIB are collections of related objects, defined in MIB modules.</div></div> <div>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1961.</div> <div>See also Arista User Manual v. 4.12.3 (7/17/13), at 1651; Arista User Manual, v. 4.11.1 (1/11/13), at 1339; Arista User Manual v. 4.10.3 (10/22/12), at 1105; Arista User Manual v. 4.9.3.2 (5/3/12), at 861; Arista User Manual v. 4.8.2 (11/18/11), at 673; Arista User Manual v. 4.7.3 (7/18/11), at 529.</div>	Dkt. 419-10 at PDF p. 210								

Cisco's Documentation	Arista's Documentation	Supporting Evidence In The Record
<div data-bbox="65 289 877 378"> <div>show snmp group</div> <div>Displays the names of configured SNMP groups, the security model being used, the status of the different views, and the storage type of each group.</div> </div> <p>Cisco IOS SNMP Support Command Reference (2013), at 123.</p>	<div data-bbox="953 289 1816 406"> <div>show snmp group</div> <div>The show snmp group command displays the names of configured SNMP groups along with the security model, and view status of each group.</div> </div> <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1971</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1669; Arista User Manual, v. 4.11.1 (1/11/13), at 1356; Arista User Manual v. 4.10.3 (10/22/12), at 1123; Arista User Manual v. 4.9.3.2 (5/3/12), at 879; Arista User Manual v. 4.8.2 (11/18/11), at 687; Arista User Manual v. 4.7.3 (7/18/11), at 543.</p>	Dkt. 419-10 at PDF p. 211
<div data-bbox="65 716 877 805"> <div>show snmp view</div> <div>Displays the family name, storage type, and status of an SNMP configuration and associated MIB.</div> </div> <p>Cisco IOS SNMP Support Command Reference (2013), at 123.</p>	<div data-bbox="953 716 1816 841"> <div>show snmp view</div> <div>The show snmp view command displays the family name, storage type, and status of a Simple Network Management Protocol (SNMP) configuration and the associated MIB. SNMP views are configured with the snmp-server view command.</div> </div> <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1986.</p> <p>See also Arista User Manual v. 4.13.6F (4/14/2014), at 1914; Arista User Manual v. 4.12.3 (7/17/13), at 1676; Arista User Manual, v. 4.11.1 (1/11/13), at 1361; Arista User Manual v. 4.10.3 (10/22/12), at 1128; Arista User Manual v. 4.9.3.2 (5/3/12), at 884; Arista User Manual v. 4.8.2 (11/18/11), at 692; Arista User Manual v. 4.7.3 (7/18/11), at 548.</p>	Dkt. 419-10 at PDF p. 211